WHAT IS CLAIMED IS:

1. A Personal Identification Number (PIN) verification apparatus comprising:

a plurality of cipher blocks linked in a Cipher Block Chain (CBC) and keyed with a secret PIN Verification Key (PVK);

a first input block coupled to a first cipher block in the CBC chain capable of receiving a text block derived from a secret Personal Identification Number (PIN); and

a second input block coupled to a second cipher block in the CBC chain capable of receiving a text block derived from a non-secret entity-identifier and ciphertext from a cipher block in the CBC chain.

2. The apparatus according to Claim 1 further comprising:

a logical operator that exclusive-ORs the plaintext block derived from the secret PIN with an initialization vector to produce an initialized block;

a first encryptor that encrypts the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block;

a logical operator that exclusive-ORs the plaintext block derived from the non-secret entity-identifier with the first ciphertext block to produce a chained block; and

a second encryptor that encrypts the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block.

3. The apparatus according to Claim 2 wherein:

the PIN verification apparatus operates in a reversible mode that enables recovery of the secret PIN from the second ciphertext block.

4. The apparatus according to Claim 2 further comprising:

a logical operator that exclusive-ORs the first ciphertext block with the second ciphertext block to produce a third ciphertext block.

5. The apparatus according to Claim 4 wherein:
the PIN verification apparatus operates in an irreversible mode that obstructs recovery of the secret PIN.

6. The apparatus according to Claim 5 further comprising:
an escrow storage coupled to the second encryptor and capable of storing the second ciphertext block.

7. The apparatus according to Claim 1 further comprising:
the plurality of cipher blocks that encrypt data according to a triple Data Encryption Standard (3-DES).

8. The apparatus according to Claim 1 further comprising:
a format converter coupled to a cipher block in the CBC chain and capable of converting hexadecimal digit ciphertext to a decimal result by scanning the hexadecimal digit ciphertext, selecting a predetermined number of numeric digits, and generating output digits as a PIN Verification Value (PVV).

9. The apparatus according to Claim 1 further comprising:
the plurality of cipher blocks that encrypt data according to a definition selected from among a group consisting of triple Data Encryption Standard (3-DES) and Advanced Encryption Standard (AES) definition.

10. The apparatus according to Claim 1 further comprising:
a first formatter configured to construct a first incoming plaintext block from a concatenation of a length digit, x hexadecimal digits of the secret Personal Identification Number (PIN) with 16-(x+1) rightmost hexadecimal digits of the non-secret entity-identifier; and
a second formatter configured to construct a second incoming plaintext block from a concatenation of y hexadecimal digits of the non-secret entity-identifier with a pad character that is repeated 16-y times.

11. A method for Personal Identification Number (PIN) verification comprising:

linking a plurality of cipher blocks in a Cipher Block Chain (CBC);

applying an incoming plaintext block derived from a secret Personal Identification Number (PIN) to one of the plurality of cipher blocks;

applying an incoming plaintext block derived from a non-secret entity-identifier and ciphertext from a cipher block in the CBC chain;

keying the plurality of cipher blocks with a secret PIN Verification Key (PVK); and

executing the cipher blocks resulting in generation of ciphertext.

12. The method according to Claim 11 further comprising:

a plurality of cipher blocks that encrypt data according to a triple Data Encryption Standard (3-DES).

13. The method according to Claim 11 wherein the PIN verification method is capable of operating in a reversible mode that enables recovery of the secret PIN, the method comprising:

exclusive-ORing the plaintext block derived from the secret PIN with an initialization vector to produce an initialized block;

encrypting the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block;

exclusive-ORing the plaintext block derived from the non-secret entity-identifier with the first ciphertext block to produce a chained block;

encrypting the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block; and

supplying the second ciphertext block for PIN verification.

14. The method according to Claim 11 wherein the PIN verification method is capable of operating in an irreversible mode that obstructs recovery of the secret PIN, the method comprising:

exclusive-ORing the plaintext block derived from the secret PIN with an initialization vector to produce an initialized block;

encrypting the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block;

exclusive-ORing the plaintext block derived from the non-secret entity-identifier with the first ciphertext block to produce a chained block;

encrypting the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block;

exclusive-ORing the first ciphertext block with the second ciphertext block to produce a third ciphertext block; and

supplying the second ciphertext block for PIN verification.

15. The method according to Claim 14 further comprising:

storing the second ciphertext block in at least one escrow to facilitate recovery of the secret PIN.

16. The method according to Claim 11 further comprising:

converting hexadecimal digit ciphertext generated by a final ciphertext block in the Cipher Block Chain (CBC) to a decimal result by scanning the hexadecimal digit ciphertext, selecting a predetermined number of numeric digits, and generating output digits as a PIN Verification Value (PVV); and

using the PVV for PIN verification.

17. The method according to Claim 11 further comprising:

supplying hexadecimal digit ciphertext generated by a final ciphertext block in the Cipher Block Chain (CBC) as a PIN Verification Value (PVV).

18. The method according to Claim 11 further comprising:

a plurality of cipher blocks that encrypt data according to a definition selected from among a group consisting of triple Data Encryption Standard (3-DES) and Advanced Encryption Standard (AES) definition.

19. The method according to Claim 11 further comprising:

constructing a first incoming plaintext block from a concatenation of a length digit, x hexadecimal digits of the secret Personal Identification Number (PIN) with 16-(x+1) rightmost hexadecimal digits of the non-secret entity-identifier; and

constructing a second incoming plaintext block from a concatenation of y hexadecimal digits of the non-secret entity-identifier with a pad character that is repeated 16-y times.

20. A data security apparatus comprising:

an enrollment terminal capable of accepting a magnetic stripe card storing a non-secret entity-identifier and an entity-selected secret Personal Identification Number (PIN);

a processor coupled to the enrollment terminal and capable of receiving the entity-identifier and the PIN; and

a memory coupled to the processor and having a computable readable program code embodied therein capable of causing the processor to enroll a PIN comprising linking a plurality of cipher blocks in a Cipher Block Chain (CBC), applying an incoming plaintext block derived from the secret Personal Identification Number (PIN) to one of the plurality of cipher blocks, applying an incoming plaintext block derived from the non-secret entity-identifier and ciphertext from a cipher block in the CBC chain, keying the plurality of cipher blocks with a secret PIN Verification Key (PVK), and executing the cipher blocks resulting in generation of ciphertext PIN Verification Value (PVV) for usage in performing a subsequent PIN verification function.

21. The apparatus according to Claim 20 wherein the PIN verification function is capable of operating in a reversible mode that enables recovery of the secret PIN and the memory further comprises:

a computable readable program code capable of causing the processor to exclusive-OR the plaintext block derived from the secret PIN with an initialization vector to produce an initialized block;

a computable readable program code capable of causing the controller to encrypt the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block;

a computable readable program code capable of causing the controller to exclusive-OR the plaintext block derived from the non-secret entity-identifier with the first ciphertext block to produce a chained block;

a computable readable program code capable of causing the controller to encrypt the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block; and

a computable readable program code capable of causing the controller to supply the second ciphertext block for PIN verification.

22. The apparatus according to Claim 20 wherein the PIN verification function is capable of operating in an irreversible mode that obstructs recovery of the secret PIN and the memory further comprises:

a computable readable program code capable of causing the processor to exclusive-OR the plaintext block derived from the secret PIN with an initialization vector to produce an initialized block;

a computable readable program code capable of causing the controller to encrypt the initialized block using triple Data Encryption Standard (3-DES) encryption to produce a first ciphertext block;

a computable readable program code capable of causing the controller to exclusive-OR the plaintext block derived from the non-secret entity-identifier with the first ciphertext block to produce a chained block;

a computable readable program code capable of causing the controller to encrypt the chained block using triple Data Encryption Standard (3-DES) encryption to produce a second ciphertext block;

a computable readable program code capable of causing the controller to exclusive-OR the first ciphertext block with the second ciphertext block to produce a third ciphertext block; and

a computable readable program code capable of causing the controller to supply the second ciphertext block for PIN verification.

23. The apparatus according to Claim 22 further comprising:

an escrow storage communicatively coupled to the transaction system and comprising at least one escrow storage element; and

the memory further comprises a computable readable program code capable of causing the processor to store the second ciphertext block in the escrow storage in at least one secret escrow share to facilitate recovery of the secret PIN.

24. The apparatus according to Claim 20 wherein the memory further comprises:

a computable readable program code capable of causing the processor to convert hexadecimal digit ciphertext generated by a final ciphertext block in the Cipher Block Chain (CBC) to a decimal result by scanning the hexadecimal digit ciphertext, selecting a predetermined number of numeric digits, and generating output digits as a PIN Verification Value (PVV); and

a computable readable program code capable of causing the processor to write the PVV to a magnetic stripe card or a smart card.

25. The apparatus according to Claim 20 wherein the memory further comprises:

a computable readable program code capable of causing the processor to store hexadecimal digit ciphertext generated by a final ciphertext block in the Cipher Block Chain (CBC) as a PIN Verification Value (PVV) in a storage element.

26. The apparatus according to Claim 20 wherein:

the plurality of cipher blocks encrypt data according to a definition selected from among a group consisting of triple Data Encryption Standard (3-DES) and Advanced Encryption Standard (AES) definition.

27. The apparatus according to Claim 20 wherein the memory further comprises:

a computable readable program code capable of causing the processor to construct a first incoming plaintext block from a concatenation of a length digit and x hexadecimal digits of the secret Personal Identification Number (PIN) with 16-(x+1) rightmost hexadecimal digits of the non-secret entity-identifier; and

a computable readable program code capable of causing the processor to construct a second incoming plaintext block from a concatenation of y hexadecimal digits of the non-secret entity-identifier with a pad character that is repeated 16-y times.

28. A data security apparatus comprising:

a PIN Verification Value (PVV) database capable of storing a plurality of PIN Verification Values (PVVs) for enrolled magnetic stripe cards;

an escrow capable of storing a plurality of escrow values associated with at least some of the enrolled magnetic stripe cards; and

a processor coupled to the PVV database and the escrow and capable of receiving an entity-identifier, a PIN Verification Value (PVV) associated to the entity-identifier, and at least one escrow value associated to the entity-identifier; and

a memory coupled to the processor and having a computable readable program code embodied therein capable of causing the processor to recover a PIN comprising linking a plurality of cipher blocks in a Cipher Block Chain (CBC), applying an incoming plaintext block derived from the PIN Verification Value (PVV) to one of the plurality of cipher blocks, applying an incoming plaintext block derived from the non-secret entity-identifier and ciphertext from a cipher block in the CBC chain, keying the plurality of cipher blocks with a secret PIN Verification Key (PVK), executing the cipher blocks to produce a ciphertext value, and combining the ciphertext value with the at least one escrow value resulting in recovery of the PIN verification function.

29. A data security apparatus comprising:

a transaction terminal capable of accepting a magnetic stripe card storing a non-secret entity-identifier and an entity-entered secret Personal Identification Number (PIN');

a PIN Verification Value (PVV) database;

a processor communicatively coupled to the transaction terminal and capable of receiving the entity-identifier, the PIN', and coupled to the PVV database and capable of retrieving a PIN Verification Value (PVV) associated with the entity-identifier; and

a memory coupled to the processor and having a computable readable program code embodied therein capable of causing the processor to verify the PIN' comprising linking a plurality of cipher blocks in a Cipher Block Chain (CBC), applying an incoming plaintext block derived from the secret entered Personal Identification Number (PIN') to one of the plurality of cipher blocks, applying an incoming plaintext block derived from the non-secret entity-identifier and ciphertext from a cipher block in the CBC chain, keying the plurality of cipher blocks with a secret PIN Verification Key (PVK), executing the cipher blocks resulting in generation of ciphertext transaction PIN Verification Value (PVV'); comparing the generated PVV' and the retrieved PVV; and determining PIN verification based on the comparison.

30. A transaction system comprising:

a network;

a plurality of servers and/or hosts coupled to the network;

a plurality of terminals coupled to the servers via the network;

a plurality of magnetic stripe cards enrolled in the transaction system and capable of insertion into the on-line terminals and performing transactions via the servers; and

a plurality of processors distributed among the servers, hosts, and/or the terminals, at least one of the processors being capable of executing PIN verification using a magnetic stripe card and having a computable readable program

code embodied therein capable of causing the processor to link a plurality of cipher blocks in a Cipher Block Chain (CBC), apply an incoming plaintext block derived from a secret Personal Identification Number (PIN) to one of the plurality of cipher blocks, apply an incoming plaintext block derived from a non-secret entity-identifier and ciphertext from a cipher block in the CBC chain, key the plurality of cipher blocks with a secret PIN Verification Key (PVK), and execute the cipher blocks resulting in generation of ciphertext.

31. A data security apparatus comprising:

means for enrolling a transaction card in a data system; and

means for generating a Personal Identification Number (PIN) Verification Value (PVV) for usage in Personal Identification Number (PIN) verification further comprising:

means for linking a plurality of cipher blocks in a Cipher Block Chain (CBC);

means for applying an incoming plaintext block derived from a secret Personal Identification Number (PIN) to one of the plurality of cipher blocks;

means for applying an incoming plaintext block derived from a non-secret entity-identifier to another of the plurality of cipher blocks;

means for keying the plurality of cipher blocks with a secret PIN Verification Key (PVK); and

means for generating a PIN Verification Value (PVV) via operation of a plurality of cipher blocks in the Cipher Block Chain; and

means for writing the PVV to a transaction card for subsequent PIN verification.